РАЗРАБОТКА МОДЕЛИ ВЫЯВЛЕНИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ С ИСПОЛЬЗОВАНИЕМ АБСТРАКТНОГО АВТОМАТА МИЛИ

канд. техн. наук, доц. С.Ю. Гавриленко, студент В.В. Челак, НТУ "ХПИ", г. Харьков

Задача оперативного выявления аномального поведения компьютерной системы в условиях вирусных атак является актуальной, так как вирусы наносят убытки на десятки миллиардов долларов [1, 2].

В докладе рассмотрена модель анализатора вредоносного программного обеспечения на основе абстрактного автомата Мили [3].

Принцип работы модели заключается в проверке возможных сред обитания вирусов и выявлении в них команд (групп команд), характерных для вирусов. Каждая из подозрительных команд сопоставляется с множеством состояний *S*. Так как функция выходов автомата Мили зависит от двух аргументов: входного сигнала и текущего состояния, то граф-схема переходов автомата сформирована так, чтобы отрабатывалась каждая ветвь алгоритма функционирования автомата.

Эвристические анализаторы при обнаружении "подозрительных" команд в файлах или загрузочных секторах выдают сообщение о возможном заражении. Введение дополнительных переходов и зацикленность на состояниях позволяют обнаружить модификацию известных вирусов.

Для идентификации состояния компьютерной системы в условиях вирусных атак была разработана программная модель, позволяющая обнаружить вирусы типа "червь" и их модификации.

Полученные результаты подтвердили возможность использования эвристического анализатора на основе абстрактного автомата Мили как дополнительного средства для выявления вирусных атак в общей системе обнаружения вредоносного программного обеспечения.

Список литературы: **1.** *Шелухин О.И.* Обнаружение вторжений в компьютерные сети / О.*И. Шелухин, Д. Ж Сакалема, А.С. Филинова*. – М.: Гарячая линия-Телеком, 2013. – 220 с. **2.** *Гошко С.В.* Технологии борьбы с компьютерными вирусами / *С.В. Гошко*. – М.: Солон-Пресс, 2009. – 352 с. **3.** *Гавриленко С.Ю.* Логіка дискретних автоматів / *С.Ю. Гавриленко, А.М. Клименко, В.І. Носков.* – Х.: НТУ "ХПІ", 2014. – 129 с.